Current Developments in Wi-Fi Liability and Regulation

Robert V. Hale II, Esq.

Saturday, October 7, 2006
Hottest Issues in Cyberspace Law
Cyberspace Committee, Business Law Section
State Bar of California

Robert V. Hale
Senior Counsel
HSBC Card Services
1441 Schilling Place
Salinas, CA 93901
831-772-6904
Robert.v.hale@us.hsbc.com

Robert V. Hale serves as Senior Counsel for HSBC Card Services, where he handles consumer, transactional, regulatory and litigation matters. Prior to joining HSBC in 2006, he was with Providian Financial Corporation (now Washington Mutual Card Services) for 8 years where his work encompassed a variety of areas, including corporate finance, technology transactions, customer marketing and operations, as well as information security.

He serves on the Financial Institutions Committee and as an advisor to the Cyberspace Committee of the Business Law Section of the California Bar. He is also the current Chair of the Corporate Law Section of the San Francisco Bar Association. He regularly publishes articles and conducts presentations on technology and banking law topics, including information security and developing technologies. He also serves as Executive Managing Editor of the Journal of Internet Law (Aspen Publishers).

Mr. Hale earned his J.D. from the University of San Francisco School of Law and is an active member of the California.

This presentation is based, in part, on a recently published article. See, Robert V. Hale, Wi-Fi Access and Operation Liability, The SciTech Lawyer, Vol. 2, Issue 4, Spring 2006, American Bar Assoc. The views expressed in this presentation are the author's own and do not necessarily reflect those of any past or present employer or client.

Overview

- Accessing and Operating Wireless Internet
  - Accessing Another's Wireless Signal
    - CFAA
    - Intercepting a Wireless Signal
      - ECPA
    - Trespass to Chattels, Theft of Services
  - Access Point Liability
  - Avoiding Liability
- Regulatory Issues
  - Municipal Wi-Fi
  - Broadband Competition

Current Developments in Wi-Fi Liability and Regulation

- Accessing Another's Wireless Signal
  - CFAA
  - Intercepting a Wireless Signal
    - ECPA
  - Trespass to Chattels, Theft of Services
- Access Point Liability
- Avoiding Liability

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –CFAA

- The Computer Fraud and Abuse Act ("CFAA") makes punishable whoever "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains … information from any protected computer if the conduct involved interstate or foreign communication."
  - To date, the Justice Department has reported at least one CFAA prosecution involving Wi-Fi. In *U.S. v. Salcedo*, the defendants hacked into the computer system of a retail store through an unsecured Wi-Fi network to steal credit card information while sitting in a car in the parking lot of the store.
- Another section of the CFAA makes punishable whoever "intentionally accesses a protected computer without authorization and, as a result of such conduct, recklessly causes damage."
- The Act also provides for a private right of action for individuals damaged by computer fraud. In each case, the statute defines "protected computer" broadly to cover essentially any computer connected to the Internet.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –CFAA

- Defining "intentional access without authorization."
  - "Access" refers to the intent to access, not the intent to damage the protected computer.
  - The user interface on Wi-Fi equipped devices typically lists detectable access points automatically by a name the WAP ("wireless access point") owner designates.
    - In a residential area, the WAP name may refer to a neighbor's last name, such as in "Jones Family Access Point."
    - The act of choosing an access point in this context could provide evidence of intentional access.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –CFAA

- The CFAA does not define "without authorization" or what it means to exceed authorization.
- Under CFAA case law, establishing unauthorized access or lack of authorization has involved reference to the means of access or its purpose.
- Courts have also found unauthorized access through a "Terms of Service" violation, even where the defendant did not receive notice of the terms.
  - *America Online v. LCGM*

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –CFAA

- At least one other court has held that a plaintiff can establish a lack of authorization through the use of an "explicit statement on the website restricting access."
  - In *EF Cultural Travel v. Zefer*, involving a defendant who used a scraper tool to extract data from a competitor's website in order to underbid projects, the court also recognized that:
    - A lack of authorization could exist implicitly, rather than explicitly in the form of a statement.
  - For example, the court noted that "password protection itself normally limits authorization by implication (and technology), even without express terms."
- Of particular relevance to the Wi-Fi context, the court found an implicit lack of authorization, rejecting the view that there exists a "presumption" of open access to the Internet.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal – CFAA

- Under *Zefer*, lack of authorization can depend on whether or not the WAP owner has implemented some procedure for gaining access to the wireless network.
  - Absence of password protection, or a similar failure to take reasonable safeguards against unauthorized use, such as encryption, may rebut the view that any outside access to a private WLAN constitutes unauthorized access.
- Still, under the presumption in *Zefer* that the end user's default status in cyberspace remains "unauthorized" until governed by either explicit or implicit agreements that grant access, the end user's initial act of choosing an access point without permission, as described above, could constitute unauthorized access in itself.
- Further complications
  - Of 88,122 WAPs scanned in 2003, 67% had not enabled security measures. A more recent survey estimates that some 80% of U.S. residential WLANs will classify as "unsecured' by 2007.
  - Signal-boosting technology that allows WAP users to expand the range ofWi-Fi signals, which can in some cases provide access nearly 75 miles away to aWAP with a normal range of 300 feet.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal – Intercepting a Wireless Signal

- Electronic Communications Privacy Act (ECPA) elements:
  - An individual must: (1) intentionally (2) intercept, endeavor to intercept, or procure another person to intercept (3) the contents of (4) an electronic communication (5) using a device. As with the CFAA, a court could apply these elements to the context of unauthorized Wi-Fi access quite easily.
- Again, most systems provide notice in some form making unauthorized access intentional to the extent that the user receives the notice.
  - The user then intercepts the wireless signal by accessing it and inevitably receives the contents of an electronic communication through receipt of standard IP packets.
- As with the CFAA, prosecutors tend to focus application of the ECPA to specific intent crimes, such as accessing another's WAP for the purpose of eavesdropping, rather than simply using another's bandwidth.
  - However, as Wi-Fi use proliferates and plaintiffs begin emerging with claims, attorneys should expect to see a variety of theories, given the unusual combination of elements that wireless Internet access presents.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –Trespass to Chattels

- Under California law, an action for trespass to chattels arises when an intentional interference with the possession of personal property causes injury.
- Courts have found the basic elements of trespass to chattels (with the exception of damages) satisfied in many different types of unauthorized computer access cases.
  - In *Intel v. Hamidi*, the court held that trespass to chattels in California "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning."
  - The court offered relevant examples of what has constituted damages in other cases involving unauthorized computer access, including overburdening or interference with the efficient functioning of computer systems and threatened harm in the potential for others to imitate the defendant's activity.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –Trespass to Chattels

- Damages -- Overburdening or interference
  - A neighbor's teenager using another neighbor's Wi-Fi to download large media files to play video games could result in overburdening or interference with the efficient functioning of the neighbor's computer system, especially involving the speed of data transfer.
  - Another increasingly probable scenario involves the use of VoIP in the same context, where a neighbor could make phone calls using another's wireless access point.
- Damages – Threatened Harm
  - It seems likely that the trespassing teenager would share his discovery with friends in the neighborhood about the "free" wireless Internet access available down the block.
    - This might in turn encourage threatened harm in the potential for others to imitate the defendant's activity, which, at least under California law, may provide the basis for an injunction against the defendant.
    - P2P implications.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –Trespass to Chattels

Defenses -- Apparent consent

- Reasonable person standard -- Under the Restatement, "[i]f words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact."
  - Lack of log-in procedures, encryption, or other forms of security may create a privilege in the would-be trespasser of apparent consent to use another's Wi-Fi network.
  - Seems plausible under a reasonable person standard given the fact that Wi-Fi routers usually come equipped with safeguards, such as log-in procedures and encryption, that the owner can choose whether or not to deploy.
  - A regular Wi-Fi user, whose laptop may automatically detect the presence of a WLAN, would come to expect to find such safeguards in place, and then, not seeing these protections, reasonably assume that the plaintiff WLAN owner has granted some form of apparent consent.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal –Trespass to Chattels

- Defenses --Apparent consent
  - Custom -- According to Prosser "[t]he defendant's privilege is limited to the conduct to which the plaintiff consents, or at least to acts of a substantially similar nature." Here, a court may turn to custom to help determine whether a scope of privilege rebuttal applies in this context.
    - For instance, the defendant could cite evidence that those who piggy-back off of other's WLANs typically do so only to perform relatively un-obtrusive Internet activities, such as checking e-mail or surfing Web pages.
    - In turn, plaintiff can cite, probably more persuasively, that those who piggy-back typically engage in activities that take-up considerable bandwidth, such as downloading music files.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal – Trespass to Chattels

- Defenses --Apparent consent
  - Custom
    - Plaintiff could also try invoking *Zefer* by arguing that the defendant's default status remains unauthorized in the absence of some form of explicit or implicit agreement.
    - In addition to rebutting this view by interpreting plaintiff's open WAP as a form of implicit agreement, defendant may then try to turn the tables by calling into question plaintiff's potential liability to his ISP for providing any open wireless Internet access to those outside plaintiff's residence.

Current Developments in Wi-Fi Liability and Regulation

Accessing Another's Wireless Signal – Theft of Services

- On April 20, 2005, Tampa Bay police arrested a man on 3rd-degree felony charges of theft of services for "hacking into" an open, residential Wi-Fi network.
- Other cases

Current Developments in Wi-Fi Liability and Regulation

Access Point Liability

- Internet service providers (ISPs) Terms of Service
  - Typically include in the written terms and conditions certain provisions that restrict service to one business or household per modem.
    - “Restricted Use. You agree not to permit anyone else to use your Member Account and that each Sub Account may only be used by one member of your household or business.” (SBC Yahoo!)
    - "[y]ou may not resell the Broadband Service, use it for high-volume purposes, or engage in similar activities that constitute resale (commercial or non-commercial), as determined solely by Verizon."
  - Assuming that ISPs police such activity, a provider could presumably terminate the contract of a customer who violates these kinds of provisions.

Current Developments in Wi-Fi Liability and Regulation

Access Point Liability

- State Telecommunications Law
  - Certain state laws may also impose liability on WAP operators who provide access in violation of ISP service terms.
    - Maryland, for example, prohibits the use of a "device, technology, [or] product … used to provide the unauthorized access to…transmission [of], or acquisition of a telecommunication service provided by a telecommunication service provider."
  - Delaware, Florida, Illinois, Michigan, Virginia and Wyoming all have laws on the books that may invoke similar liability.
    - Delaware law, for instance, prohibits “the unauthorized acquisition or theft of any telecommunication service or to receive, disrupt, transmit, decrypt, acquire or facilitate the receipt, disruption, transmission, decryption or acquisition of any telecommunication service without the express consent or express authorization of the telecommunication service provider.”

Current Developments in Wi-Fi Liability and Regulation

Access Point Liability – Vicarious/Contributory

- Wireless access operators could also incur liability to the extent that they make access available, and in doing so, facilitate activities that damage others.
  - Continuing the earlier hypothetical, if someone downloads unauthorized copies of music files using another's WLAN, and thereby commits copyright infringement, vicarious liability for the infringement may attach to the WAP operator.
- Under *Napster*, vicarious copyright infringement applies to cases where the peer-to-peer network has:
  - "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."

Current Developments in Wi-Fi Liability and Regulation

Access Point Liability --Vicarious/Contributory

- Right and ability to supervise
  - Home-run WAPs typically have no monitoring mechanisms to facilitate tracking of potentially infringing activity (assuming operators have a right to supervise such activity).
  - Ability to block certain users usually requires implementing security options that the average user would probably avoid due to complexity and lack of automation.
- Direct financial interest
  - Those who deploy Wi-Fi residentially do so primarily to make the Internet more accessible within their own homes -- unlikely to have any financial interest in infringing activities.
  - Commercial HotSpot operators
    - Infringing users may run up more access fees in their attempts to download infringing media files.
    - Prevailing reluctance to impose responsibility on ISPs for harmful conduct committed by end-users would probably protect these parties from contributory liability in this context.

Current Developments in Wi-Fi Liability and Regulation

Avoiding Liability –End user

- Don't Piggy-Back
  - Until the courts and legislatures better define the legal status of Wi-Fi arrangements, don't access others' open WLANs, absent an explicit agreement or notice.
  - If you must, then avoid heavy downloading activity (music, games, movies, etc.) that has a tendency to overburden the network and may amount to recoverable damages.
- Similarly, sapping a residential neighbor's Internet service in lieu of paying for one's own seems potentially more culpable than accessing signals in a business area while on a lunch break.
- On the other hand, those for whom piggy-backing supplies the only practicable means of obtaining residential high-speed Internet access may want to seek out services that provide Wi-Fi sharing arrangements, through which ISPs pass-through service payments from end-users on to WAP operators.

Current Developments in Wi-Fi Liability and Regulation

Avoiding Liability –WAP Operator

- Implement Security
  - Implementing a secure network through the use of password protection and encryption. To the extent that the operator can identify any interlopers, the operator should take steps to exclude such users from the network.
    - Unfortunately, as mentioned above, the difficulty involved both in securing and monitoring WLANs adds confusion to the issue of the operator's potential liability.
- Proof of damages will require evidence of unlawful activity and mitigation of such activity
  - For instance, in moving a claim forward, the plaintiff will need to provide proof that the alleged interloper accessed plaintiff's WLAN, as well as evidence of damages.
    - In doing so, the plaintiff will need to produce log files that identify the defendant and other evidence that shows the defendant's activity interrupted the network to such an extent as to justify damages.
    - Proof of implementation of security measures.

Current Developments in Wi-Fi Liability and Regulation

Update – *Salcedo* Prosecution

- On July 10th, the 4th Circuit Court of Appeals issued its opinion in *U.S. v. Salcedo*, upholding a nine-year prison term for Salcedo.
- Under the court's ruling, Salcedo will not be eligible for release until May 2011. Despite the fact that no damage was done and despite cooperating to help Lowe's boost its security after his arrest, Salcedo was sentenced to what the government described at the time as the longest U.S. prison term for a hacker in history.
- The sentence was largely based on the amount of harm that would have resulted had the plan succeeded. The court said, "We find that the district court did not err in using Salcedo's admitted intentions to harm 250 or more victims and to traffic the stolen information to enhance his sentence."
- The opinion in the case may be found at http://pacer.ca4.uscourts.gov/opinion.pdf/054147.U.pdf

Current Developments in Wi-Fi Liability and Regulation

Regulatory Issues –Municipal Wi-Fi --Overview

- The FCC's broadband policy is that all facilities-based broadband services — including broadband services provided by cable operators, incumbent local exchange carriers (ILECs), and broadband over power line (BPL) — should not be regulated either as cable services or as telecommunications services, but as information services, subject to minimal federal regulation.
- Several municipalities have recently announced plans to develop Wi-Fi networks, including Philadelphia and San Francisco.
  - EarthLink obtained the contract for Philadelphia and plans to charge residents $20 per month, and $10 for low-income residents, with speeds of about 1MB per second (about ¼ the speed of most cable broadband connections).
  - Verizon and SBC now sell broadband for as little as $14.95 a month, 25% less than EarthLink's Philadelphia rate. Cable companies bundle broadband with VoIP and televisions services.

Current Developments in Wi-Fi Liability and Regulation

Regulatory Issues – Municipal Wi-Fi -- Federal Legislation

For

- Community Broadband Act of 2005 (S.1294)
  - Amends the Telecommunications Act of 1996 to prohibit any state statute, regulation, or other legal requirement from prohibiting any public provider from providing, to any person or public or private entity, advanced telecommunications capability or any service that utilizes such capability.
- Policy arguments
  - Some state laws prohibit such activity
  - Main concern is rural areas under-served by ISPs.

Current Developments in Wi-Fi Liability and Regulation

Regulatory Issues – Municipal Wi-Fi -- Federal Legislation

Against

- Broadband Investment and Consumer Choice Act (S. 1504)
  - A bill to establish a market driven telecommunications marketplace, to eliminate government managed competition of existing communication service, and to provide parity between functionally equivalent services.
- Preserving Innovation in Telecom Act of 2005 (H.R.2724)
  - Amends the Communications Act of 1934 to prohibit any state or local government, or an entity affiliated with either government, from providing any telecommunications, information, or cable service in any geographic area within such government in which a corporation or other private entity not affiliated with such government is offering a substantially similar service.
- Policy arguments
  - Publicly sanctioned services could deter the Bells and cable companies from investing in their own networks.

Current Developments in Wi-Fi Liability and Regulation

Regulatory Issues – Municipal Wi-Fi –FCC

- Continental Airlines recently filed a petition with the FCC seeking a ruling on whether Wi-Fi antennas are protected under the FCC's Over-the-Air Reception Devices (OTARD) rules, which prohibit certain restrictions to receive wireless signals.
  - The Massachusetts Port Authority demanded that Continental cease operating its Wi-Fi hotspot within the premises of its frequent flyer lounge, which Continental argued is impermissibleunder the OTARD rules.
    - The FCC's decision will impact lessees' and lessors' rights with respect to installing Wi-Fi equipment on leased premises.